Trustwave®

Trustwave Proactive Threat Hunting

IDENTIFY ACTIVE THREATS AND OPEN THREAT VECTORS IN YOUR ENVIRONMENT.

Benefits

- Reduce attacker dwell time
- Detect unknown threats in your environment
- Maximize visibility into open threat vectors across your environment
- Gain peace of mind and a partner
- Mitigate risk to your organization and customers

Blocking an attacker at the perimeter will not always be successful. Threats will continue to bypass preventative security controls. Trustwave Proactive Threat Hunting helps you fortify your security defenses by identifying hidden attackers in your environment and open threat vectors that can lead to a breach.

What we do is different

People are at the core of threat hunting and central to the practice. Automated threat hunting has its value but requires an indicator of compromise (IOC) and tactics, techniques, and procedures (TTPs) to be built into a security tool for it to look for an indication of adversary presence.

Unlike other threat hunting services which only use automated, indicator-centric detection methods, Trustwave Proactive Threat Hunting is human-led with a creative focus on clues and hypotheses. Our approach to threat hunting combines human-driven and automated process with supported technologies in your existing environment and our purpose-built threat hunting capabilities to help you get ahead of adversaries.

How we do it

Threat hunting starts from one of two points: a fact or finding, or a hypothesis. A fact or finding could be the output of an automated tool or system trying to create a finding. Many in the industry equate the output from the system to be “automated threat hunting”. Trustwave starts threat hunting from this point.

Trustwave Proactive Threat Hunting leverages a cadre of renowned Trustwave SpiderLabs threat hunters, a proprietary threat hunting platform and best practice recommendations to help you eliminate threats in your environment. Our mission is to identify insider threat actors, unpatched vulnerabilities, network or software misconfigurations, and advanced persistent threats dwelling in your security environment.

An elite group of threat hunters – Trustwave SpiderLabs®

Artificial intelligence alone is not a replacement for human expertise and experience. The Trustwave SpiderLabs team of threat hunters is composed of experts with hybrid domain expertise and defensive mindsets spanning diverse security career experiences.

- Career experience ranging from Corporate Information Security to Security Research to Federal and Local Law Enforcement
- Decades of experience in incident response, digital forensics, cyber threat intelligence and malware analysis
- Hands-on experience conducting hundreds of threat hunts and investigations where they have encountered adversaries and honed creative thinking skills

Purpose-built threat hunting capabilities

When you partner with Trustwave SpiderLabs for a proactive threat hunt, our expert hunters will employ our proprietary Threat Hunting Platform, combined with your supported security tools in your existing environment and Trustwave SpiderLabs cyber threat intelligence to find threats and weaknesses within your network infrastructure.

- Trustwave Threat Hunting Platform consists of five elements: Agent Hunter, Intel Hunter, Scribe, Dweller, Artifact Collector
- Leveraging industry-leading security tools, we extract the best capabilities for threat hunting to accelerate time to value
- Integrating with multiple security tools for threat hunting provides additional insights which improve context for threat hunting, mean time to detect, and mean time to respond
- Blend your data with a comprehensive threat intelligence library of Trustwave SpiderLabs original research, a large incognito clientele data set, partner intelligence and open-source intelligence

Actional findings and best-practice remediation recommendations

Trustwave believes a good threat hunt is more than identifying active attackers. Trustwave Proactive Threat Hunting delivers findings that can extend beyond endpoints to network traffic and security devices. Our findings will report environmental flaws, outdated software, network misconfigurations. And when we find a threat, we work with you to take a response action. We deliver clear action items, prioritized by threat level, and designed to improve your overall security posture.

If active attackers are identified, you can leverage Trustwave Digital Forensics & Incident Response (DFIR) experts to handle a breach response investigation. We also provide you a seamless transition into our broader portfolio of Managed Threat Detection and Response services like Managed Detection and Response Complete, which includes continuous threat hunting. This type of hunting occurs multiple times per year and each iteration becomes more laser focused on anomaly detection.

Case Study

Healthcare

Situation

Following a business acquisition, client was merging systems, devices, and networks

Discovery

During a Proactive Threat Hunt Engagement, threat hunters found over 100 files containing passwords in clear text. Some of the file names were Passwords.txt, Shared-passwords.xls, mypasswords.txt, etc. Many of these passwords were for mission critical healthcare applications.

Threat

Upon entry, attackers do not immediately know where critical assets are. Easy to find files containing passwords are equivalent to giving the thief the keys.

Outcome

- Recommendation was made to remove the files and enforce password managers.
- Mitigated the risk of data exploitation and potential HIPPA violations.

For more information on these and other Trustwave products and services, visit www.trustwave.com

Trustwave®

www.trustwave.com